

(19) RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

(11) N° de publication :
(à n'utiliser que pour les
commandes de reproduction)

2 753 859

(21) N° d'enregistrement national : 96 11914

(51) Int Cl⁶ : H 04 L 9/32, H 04 M 3/42

(12)

DEMANDE DE BREVET D'INVENTION

A1

(22) Date de dépôt : 25.09.96.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : 27.03.98 Bulletin 98/13.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule.*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : FINTEL SOCIETE ANONYME — FR.

(72) Inventeur(s) : ROSSET FRANK, GAYET ALAIN et MOULIN JEAN.

(73) Titulaire(s) :

(74) Mandataire : CABINET PATRICE VIDON.

(54) PROCÉDE ET SYSTEME POUR SECURISER LES PRESTATIONS DE SERVICE DES OPERATEURS DE TELECOMMUNICATION.

(57) L'invention concerne un procédé et un système permettant à un opérateur (12) de télécommunication d'identifier de manière rapide et de débiter de manière sûre les abonnés d'un réseau téléphonique.

Le procédé comprend les étapes suivantes:

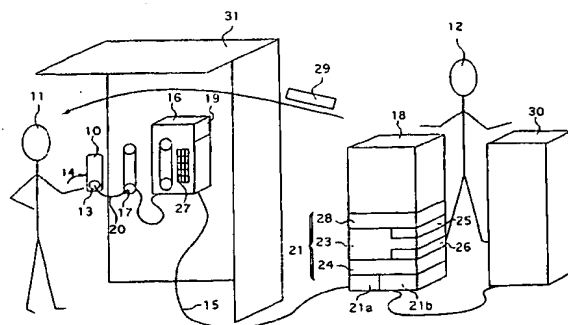
- l'opérateur (12) de télécommunication met à la disposition de chacun des abonnés (11) une carte d'abonné (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque abonné et pour chaque carte d'abonné,

- ladite carte (10), au format carte de crédit, émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, lorsqu'elle est actionnée par l'abonné (11),

- les signaux acoustiques d'identification sont reçus par le microphone (17) du combiné téléphonique et sont convertis en signaux électriques, avant d'être transmis par le réseau de communication (15) au service informatique (28) de l'opérateur de télécommunication (12),

- les signaux transmis sont traités et décryptés (29) électroniquement par le service informatique (18) de l'opérateur (12) de télécommunication et les données obtenues après traitement et décryptage sont comparées (25) aux données d'identification de l'abonné et de la carte d'abonné déte-

nues par le service informatique (18) de l'opérateur de télécommunication.



FR 2 753 859 - A1



Procédé et système pour sécuriser les prestations de service des opérateurs de télécommunication.

Le domaine de l'invention est celui des prestations de service à distance proposées par les opérateurs de télécommunication à leurs clients abonnés à leur réseau.

5 Plus précisément l'invention concerne un procédé et un système permettant à un opérateur de télécommunication d'identifier de manière rapide et de débiter de manière sûre les comptes des abonnés d'un réseau téléphonique.

10 Le problème posé est d'empêcher un utilisateur mal intentionné d'accéder au réseau de télécommunication sans y être autorisé, sans acquitter les droits correspondants ou en prétendant qu'il n'a pas demandé les services qui lui sont débités par l'opérateur de télécommunication.

15 Pour résoudre ce problème il a été proposé d'utiliser des clés d'accès générées par des cartes à mémoire et de modifier les combinés téléphoniques pour qu'ils puissent lire les cartes à mémoire. Ces solutions, outre leur coût, sont peu pratiques et longues à mettre en oeuvre. En fait, le problème posé ne peut être effectivement résolu que si on sait résoudre simultanément un autre problème : concevoir un procédé et un système commode d'utilisation, rapide à mettre en oeuvre en oeuvre et économique. En effet, dès

20 Ces objectifs sont atteints et ces problèmes sont résolus selon l'invention à l'aide d'un procédé comprenant les étapes suivantes :

- l'opérateur de télécommunication met à la disposition de chacun des abonnés une carte d'abonné, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque abonné et pour chaque carte d'abonné,
- 25 - la dite carte, au format carte de crédit, émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, lorsqu'elle est actionnée par l'abonné,
- les signaux acoustiques d'identification sont reçus par le microphone du combiné téléphonique et sont convertis en signaux électriques, avant d'être transmis par le réseau
- 30 de communication au service informatique de l'opérateur de télécommunication,

- les signaux transmis sont traités et décryptés électroniquement par le service informatique de l'opérateur de télécommunication et les données obtenues après traitement et décryptage sont comparées aux données d'identification de l'abonné et de la carte d'abonné détenues par le service informatique de l'opérateur de télécommunication.

5 Ainsi, grâce à ce procédé, l'opérateur de télécommunication peut vérifier que l'appelant dispose bien d'une carte authentique et non d'un leurre informatique. Il a pu également identifier le titulaire de la carte comme étant une personne habilitée à utiliser les services qu'il offre. De sorte qu'en cas de conformité le client est immédiatement mis en communication avec le serveur vocal ou l'opératrice de l'opérateur de télécommunications. Par ailleurs, les fraudeurs n'ont plus la possibilité de dérober les données d'identification puisque celles-ci sont transmises automatiquement sous une forme cryptée.

 Avantageusement les signaux acoustiques émis par la carte varient à chaque opération.

15 Afin d'augmenter la sécurité du procédé, dans une variante de réalisation, le procédé comprend en outre l'étape suivante : l'abonné émet, au moyen d'un clavier associé au combiné téléphonique et/ou à la carte, un code confidentiel. Après transmission au service informatique de l'opérateur de télécommunication, via le réseau de communication, ce code confidentiel est traité et comparé au code confidentiel personnel de l'abonné détenu par le service informatique de l'opérateur de télécommunication.

20 Ainsi, l'opérateur de télécommunication peut vérifier que l'appelant est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

25 Dans une autre variante de réalisation, afin également de renforcer la sécurité du procédé et d'éviter que le client ne puisse pas contester l'ordre qu'il a passé à l'opérateur de télécommunication, le procédé comprend en outre l'étape suivante :

30 - les ordres donnés par l'abonné à l'opérateur de télécommunication sont validés par l'abonné en actionnant la carte d'abonné pour qu'elle émette un signal acoustique crypté de validation

- le dit signal de validation est enregistré par le service informatique de l'opérateur de télécommunication.

Avantageusement, le procédé selon l'invention pourra comporter l'étape complémentaire suivante :

5 - un accusé de réception du signal de validation est adressé au client.

Grâce à ce procédé, l'abonné a validé, par une signature électronique, l'ordre qu'il a donné à l'opérateur de télécommunication.

10 L'invention concerne également un système permettant aux abonnés d'un réseau de télécommunication d'accéder, de manière sûre et rapide, aux services que l'opérateur de télécommunication offre à ses clients. Ce système a pour caractéristique de comprendre les moyens de mise en oeuvre du procédé ci-dessus défini et de ses variantes de réalisation.

Plus particulièrement, le système selon l'invention comprend :

15 - une carte d'abonné, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte d'abonné et pour chaque abonné, mise à la disposition de ceux-ci par l'opérateur de télécommunication. La dite carte comporte des moyens d'émission de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie. Ces moyens d'émission sont actionnés par l'abonné au moyen d'un élément accessible de l'extérieur de la carte d'abonné,

20 - un combiné téléphonique comprenant un microphone destiné à recevoir et transformer les signaux acoustiques reçus, en des signaux électroniques transmissibles à distance au moyen du - des moyens informatiques, dépendant des services informatiques de l'opérateur de télécommunication, connectés au réseau de télécommunication, les dits moyens informatiques comprenant :

25 * une base de données contenant les références des cartes d'abonné et des abonnés et leurs données d'identification,

* des moyens de traitement et de décryptage des signaux électroniques permettant d'obtenir des données caractéristiques des abonnés et des cartes d'abonné,

30 * des moyens de comparaison des données d'identification contenues dans la base de données et des données caractéristiques des abonnés et des cartes d'abonné.

De sorte qu'en cas de conformité l'abonné peut être mis en communication avec son interlocuteur et son compte d'abonné peut être débité.

5 Afin d'augmenter la sécurité du système, dans une variante de réalisation, le système comprend en outre des seconds moyens de comparaison d'un code confidentiel personnel à l'abonné contenu dans la base de données, à un code confidentiel émis par l'abonné. Ce code est émis au moyen d'un clavier associé au combiné téléphonique et/ou à la carte et transmis aux moyens informatiques de l'opérateur de télécommunication, par le réseau de communication.

10 Ainsi, l'opérateur de télécommunication peut vérifier que l'appelant est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

Dans une autre variante de réalisation, afin également de renforcer la sécurité du système et d'éviter que le client ne puisse contester l'ordre qu'il a donné à l'opérateur de télécommunication, le système selon l'invention est tel que :

- 15 - ladite carte émet, lorsqu'elle est actionnée par l'abonné, un signal acoustique crypté de validation des ordres donnés par l'abonné,
- lesdits moyens informatiques comprennent des moyens de détection et d'enregistrement du signal de validation.

20 Grâce à ce système, le client a validé, par une signature électronique, l'ordre qu'il a donné à l'opérateur de télécommunication.

Avantageusement dans ce cas les moyens informatiques comprenant en outre des moyens d'édition d'un accusé de réception des ordres donnés. Cet accusé de réception est adressé à l'abonné.

25 D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description d'une variante de réalisation de l'invention, donnée à titre d'exemple indicatifs et non limitatif, et de la figure 1 annexée présentant une vue schématique en perspective du système et du procédé selon l'invention.

30 Le système et le procédé selon l'invention permettent au client 11 d'appeler, de manière sûre et rapide, notamment d'une cabine publique 31, au moyen d'un combiné téléphonique 16 comportant un microphone 17, les services 30 que l'opérateur de

télécommunication (l'opératrice) 12 met à la disposition de ses clients 11. Le combiné téléphonique 16, situé à distance des services informatiques 18 de l'opérateur de télécommunication, est connecté aux services informatiques 18 via un réseau de communication 15.

5 Le système comprend une carte 10, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et pour chaque client 11. Cette carte est mise à la disposition des abonnés de l'opérateur de télécommunication 12. La carte 10 comporte des moyens d'émission de brefs signaux acoustiques d'identification 13, de type DTMF, cryptés au moins en partie. Ces signaux sont émis lorsque les moyens d'émission 13 sont
10 actionnés par l'abonné au moyen d'un élément 14 accessible de l'extérieur de la carte (non visible sur la figure car situé sur l'autre côté de la carte). Les signaux acoustiques 20 sont reçus par le microphone 17 du combiné téléphonique, contre lequel l'abonné accole la carte 10. Le système comprend également des moyens 19 de transmission des signaux acoustiques 20, situés dans le combiné téléphonique 16. Ces moyens de transmission
15 transmettent à distance les signaux, après traitement, via le réseau de communication 15. Le système comprend également des moyens informatiques 21, dépendants des services informatiques 18 de l'opérateur de télécommunication. Ces moyens informatiques sont connectés au réseau de communication 15 et situés à distance des combinés téléphoniques 16.

20 Ces moyens informatiques 21 comprennent eux-mêmes :

 * une base de données 23 contenant les références des cartes et des clients et leurs données d'identification,

 * des moyens de traitement et de décryptage 24 des signaux électroniques permettant d'obtenir des données caractéristiques des clients et des cartes,

25 * des moyens de comparaison 25 des données d'identification contenues dans la base de données 23 et des données caractéristiques des clients et des cartes.

De sorte qu'en cas de conformité, les services 30 de l'opérateur de télécommunication sont immédiatement accessibles au client 11.

30 De préférence les moyens de cryptage de la carte et de décryptage des services informatiques sont conçus de telle sorte que le signal acoustique varie à chaque opération

(horloge, compteur d'opérations etc., ainsi qu'il est notamment décrit dans les brevets US N° : 4,998,279 et US N° : 4,298,098). Ainsi l'enregistrement, sous quelque forme que ce soit, des signaux acoustiques ne sera d'aucune utilité à un fraudeur pour se faire identifier par les services informatiques de l'opérateur de télécommunication et bénéficier des services de celui-ci.

Afin d'augmenter la sécurité du système, dans la variante de réalisation représentée sur la figure 1, les moyens informatiques 21 comprennent en outre des seconds moyens de comparaison 26. Ces moyens de comparaison permettent de comparer un code confidentiel personnel à l'abonné, contenu dans la base de données, avec le code confidentiel émis par l'utilisateur. Ce code est émis au moyen d'un clavier 27 associé au combiné téléphonique 16 et/ou à la carte 10 et transmis aux moyens informatiques 21 de l'opérateur de télécommunication, par le réseau de communication 15.

Ainsi, l'opérateur de communication à l'assurance que l'appelant 11 est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

Dans une autre variante de réalisation, afin également de renforcer la sécurité du système et d'éviter que le client ne puisse contester l'ordre qu'il a donné à l'opérateur de télécommunication, le système selon l'invention est tel que :

- la carte 10 émet, lorsqu'elle est actionnée 14 par l'abonné, un signal acoustique crypté de validation des ordres donnés par l'abonné 11,
- lesdits moyens informatiques 21 comprennent des moyens de détection 21a et d'enregistrement 21b du signal de validation.

Grâce à ce système, le client a validé, par une signature électronique, l'ordre qu'il a donné à l'opérateur de télécommunication.

Avantageusement dans ce cas les moyens informatiques 21 comprennent en outre des moyens d'édition 28 d'un accusé de réception 29 des ordres donnés. Cet accusé de réception est adressé à l'abonné 11.

REVENDICATIONS

1. Procédé permettant à un opérateur (12) de télécommunication d'identifier de manière rapide et de débiter de manière sûre les abonnés d'un réseau téléphonique, caractérisé en ce qu'il comprend les étapes suivantes :

5 - l'opérateur (12) de télécommunication met à la disposition de chacun des abonnés (11) une carte d'abonné (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque abonné et pour chaque carte d'abonné,

 - la dite carte (10), au format carte de crédit, émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, lorsqu'elle est actionnée par
10 l'abonné (11),

 - les signaux acoustiques d'identification sont reçus par le microphone (17) du combiné téléphonique et sont convertis en signaux électriques, avant d'être transmis par le réseau de communication (15) au service informatique (28) de l'opérateur de télécommunication (12),

15 - les signaux transmis sont traités et décryptés (29) électroniquement par le service informatique (18) de l'opérateur (12) de télécommunication et les données obtenues après traitement et décryptage sont comparées (25) aux données d'identification de l'abonné et de la carte d'abonné détenues par le service informatique (18) de l'opérateur de télécommunication.

20 2. Procédé selon la revendication 1, caractérisé en ce qu'il comprend en outre l'étape suivante :

 - l'abonné émet, au moyen d'un clavier (27) associé au microphone et/ou à la carte, un code confidentiel ; après transmission au service informatique (18) de l'opérateur de télécommunication, par le réseau de communication (15), ce code confidentiel est traité
25 et comparé (26) au code confidentiel personnel du client détenu par le service informatique (18) de l'opérateur de télécommunication.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce qu'il comprend en outre l'étape suivante :

30 - les ordres donnés par l'abonné à l'opérateur de télécommunication sont validés par l'abonné en actionnant (14) la carte d'abonné (10) pour qu'elle émette un signal

acoustique crypté de validation ;

- ledit signal de validation est enregistré (21b) par le service informatique de l'opérateur de télécommunication.

4. Procédé selon la revendication 3, caractérisé en ce qu'il comprend en outre l'étape suivante :

- un accusé de réception (29) du signal de validation est adressé au client.

5. Procédé selon l'un des revendications 1 à 4 caractérisé en ce que les signaux acoustiques émis par la carte varient à chaque opération.

6. Système permettant à un opérateur de télécommunication (12) d'identifier de manière rapide et de débiter de manière sûre les abonnés (11) d'un réseau téléphonique, caractérisé en ce qu'il comprend :

- une carte d'abonné (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte d'abonné et pour chaque abonné, mise à la disposition de celui-ci ;

la dite carte comportant des moyens (13) d'émission de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, lorsque les dits moyens d'émission sont actionnés par l'abonné au moyen d'un élément (14) accessible de l'extérieur de la carte d'abonné,

- un combiné téléphonique comprenant un microphone (17) destiné à recevoir et transformer les signaux acoustiques reçus, en des signaux électroniques transmissibles à distance au moyen du réseau de communication (25),

- des moyens informatiques (21), dépendant des services informatiques (18) de l'opérateur de télécommunication (12), connectés au réseau de télécommunication (15), les dits moyens informatiques comprenant :

* une base de données (23) contenant les références des cartes d'abonné et des abonnés et leurs données d'identification,

* des moyens de traitement et de décryptage (24) des signaux électroniques permettant d'obtenir des données caractéristiques des abonnés et des cartes d'abonné,

* des moyens de comparaison (25) des données d'identification

contenues dans la base de données et des données caractéristiques des abonnés et des cartes d'abonné,

de sorte qu'en cas de conformité l'abonné peut être mis en communication avec son interlocuteur et son compte d'abonné peut être débité.

5 7. Système selon la revendication 6, caractérisé en ce que lesdits moyens informatiques comprennent en outre:

10 - des seconds moyens de comparaison (26) d'un code confidentiel personnel de l'abonné contenu dans la base de données, à un code confidentiel émis par le client au moyen d'un clavier (27) associé au combiné téléphonique et/ou à la carte et transmis aux moyens informatiques de l'opérateur de télécommunication, par le réseau de communication.

8. Système selon les revendications 6 ou 7, caractérisé en ce que ladite carte émet en outre, lorsqu'elle est actionnée (14) par l'abonné, un signal acoustique crypté de validation des ordres donnés par l'abonné,

15 et en ce que lesdits moyens informatiques comprennent en outre des moyens de détection (21a) et d'enregistrement (21b) du signal de validation.

9. Système selon la revendication 8, caractérisé en ce que lesdits moyens informatiques (18) comprennent en outre des moyens d'édition (28) d'un accusé de réception (29) des ordres donnés, destiné à être adressé à l'abonné.

20 10. Système selon l'une des revendications 6 à 9, caractérisé en ce que la carte comporte des moyens de cryptage permettant de varier les signaux acoustiques d'une opération à l'autre.

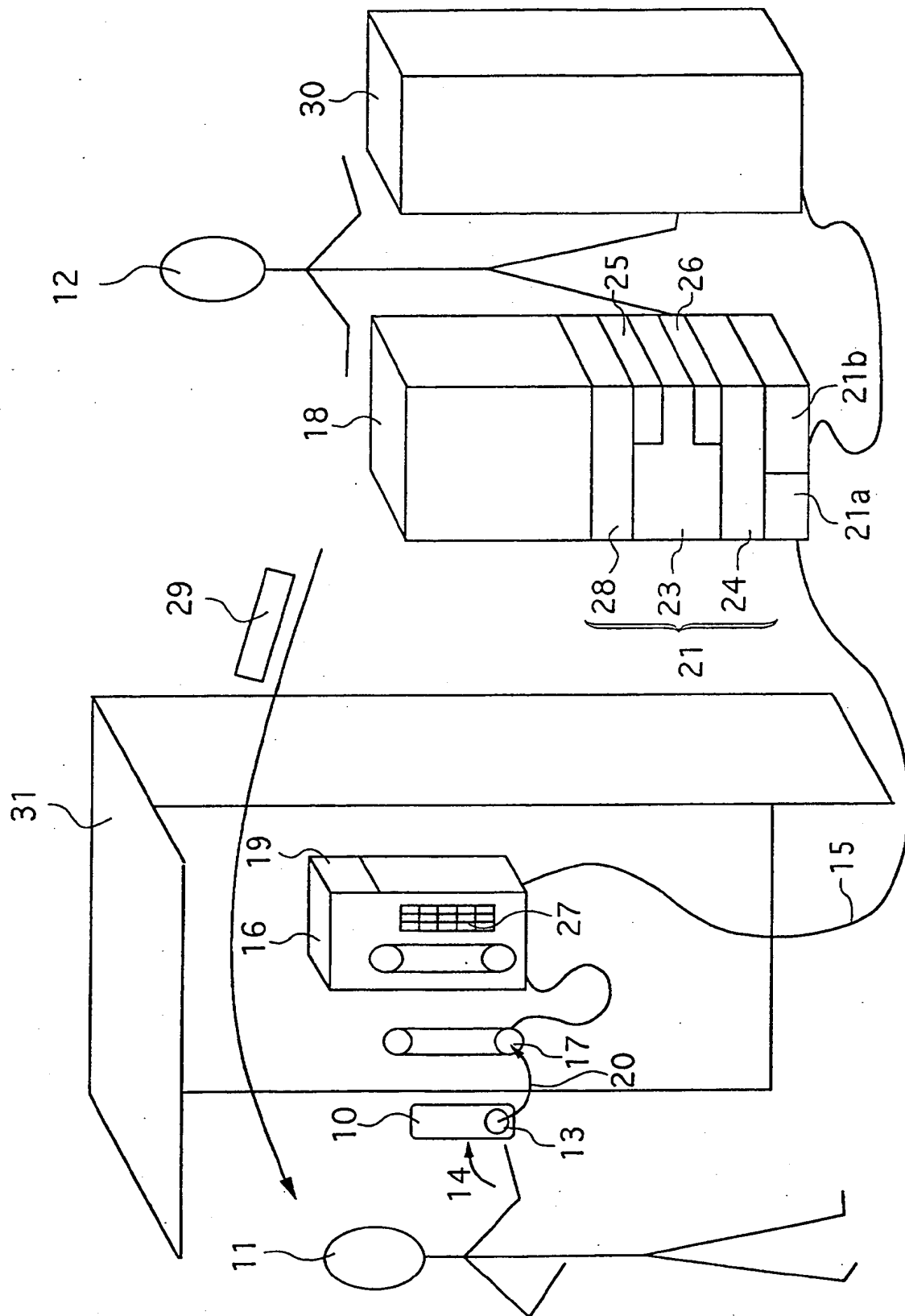


Fig. 1

INSTITUT NATIONAL
de la
PROPRIÉTÉ INDUSTRIELLERAPPORT DE RECHERCHE
PRELIMINAIRE
établi sur la base des dernières revendications
déposées avant le commencement de la rechercheFA 533650
FR 9611914

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	WO 96 04741 A (MARK ANDREW R) 15 Février 1996 * abrégé * * figures 1-7 * * page 15, ligne 17 - page 21, ligne 10 * * page 53, ligne 17 - page 62, ligne 16 * * page 69, ligne 8 - page 71, ligne 3 * * page 74, ligne 32 - page 78, ligne 11 * ---	1-4,6-10
E	WO 97 12471 A (FINTEL S A) 3 Avril 1997 * le document en entier * ---	1,2,6,7
A	WO 88 03294 A (CALL IT CO) 5 Mai 1988 * le document en entier * ---	1,2,6,7
A	WO 82 04169 A (SCHAUSE SA IND MECANICA & ELET ; SCHAUSE DONALD ELMAR (BR)) 25 Novembre 1982 * le document en entier * ---	1-4,6-10
A	BELL SYSTEM TECHNICAL JOURNAL, vol. 61, no. 7, pt.3, Septembre 1982, USA, pages 1675-1714, XP002034396 COLFALONE D E; ROGERS B W; THORNBERRY R J JR: "Calling card service-TSPS hardware, software and signalling implementation" * le document en entier * ---	1-10
A	BELL SYSTEM TECHNICAL JOURNAL, vol. 61, no. 7, pt.3, Septembre 1982, USA, pages 16655-1673, XP002034397 BASINGER R G; BERGER M; PRELL E M; RANSOM V L; WILLIAMS J R;: "Calling Card Service -Overall Description and operational Characteristics" * le document en entier * ---	1-10
		DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)
		H04M G07F H04Q
Date d'achèvement de la recherche 12 Août 1997		Examineur Megalou, M
<p>CATEGORIE DES DOCUMENTS CITES</p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons ----- & : membre de la même famille, document correspondant</p>		

3

EPO FORM 150 (12/92) (P/C13)

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	US 4 707 592 A (WARE PAUL N) 17 Novembre 1987 * abrégé * * colonne 5, ligne 39 - ligne 51 * * figures 1-7 * -----	1-10
		DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)
Date d'achèvement de la recherche		Examineur
12 Août 1997		Megalou, M
CATEGORIE DES DOCUMENTS CITES X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant		

3

EPO FORM 1503 Q1.82 (PMCL19)

THIS PAGE BLANK (USPTO)